MATH CIRCLE HOMEWORK 6

A warm-up and a review:

1. Three friends – sculptor White, violinist Black, and artist Redhead – are in a cafeteria. "It is remarkable that one of us has white hair, another has black hair, and the third red hair, though no one's name gives the color of their hair," said the black-haired person. "You are right," answered White. What color is the artist's hair?

2. A box contains 300 matches. Players take turns removing no more than half the matches in the box. The player who cannot move loses. Who has the winning strategy?

Modular stuff:

3. Show that if $2^n + 1$ is prime then n must be a power of 2. Must $2^{2^m} + 1$ be prime for every nonnegative integer m?

4. In this problem we will show that if p is prime and p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$.

(1) Let p be a prime and a a number not divisible by p. Show that none of the numbers $a, 2a, 3a, ..., (p-1)a$ are divisible by p.

(2) Let p and a be the same as above. Show that, in lowest form modulo p, the set of numbers

$$a, 2a, 3a, ..., (p-1)a \pmod{p}$$

is just a rearrangement of the numbers

$$1, 2, 3, ..., p-1.$$

(3) Show that $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. Conclude that $a^{p-1} \equiv 1 \pmod{p}$.

5. Use the previous problem to show that every number $1, 2, 3, ..., p-1$ has a multiplicative inverse, modulo p, when p is prime. That is, show that for every $x = 1, 2, 3, \ldots, p-1$, there exists an integer y so that $xy \equiv 1 \pmod{p}$.